RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: PART2-R01

Vendor Vulnerability: Get Ahead of Third-Party AI Risk

Mary Carmichael
Managing Director, Momentum Technology

Dooshima Dabo'Adzuana
Researcher, Boise State University

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

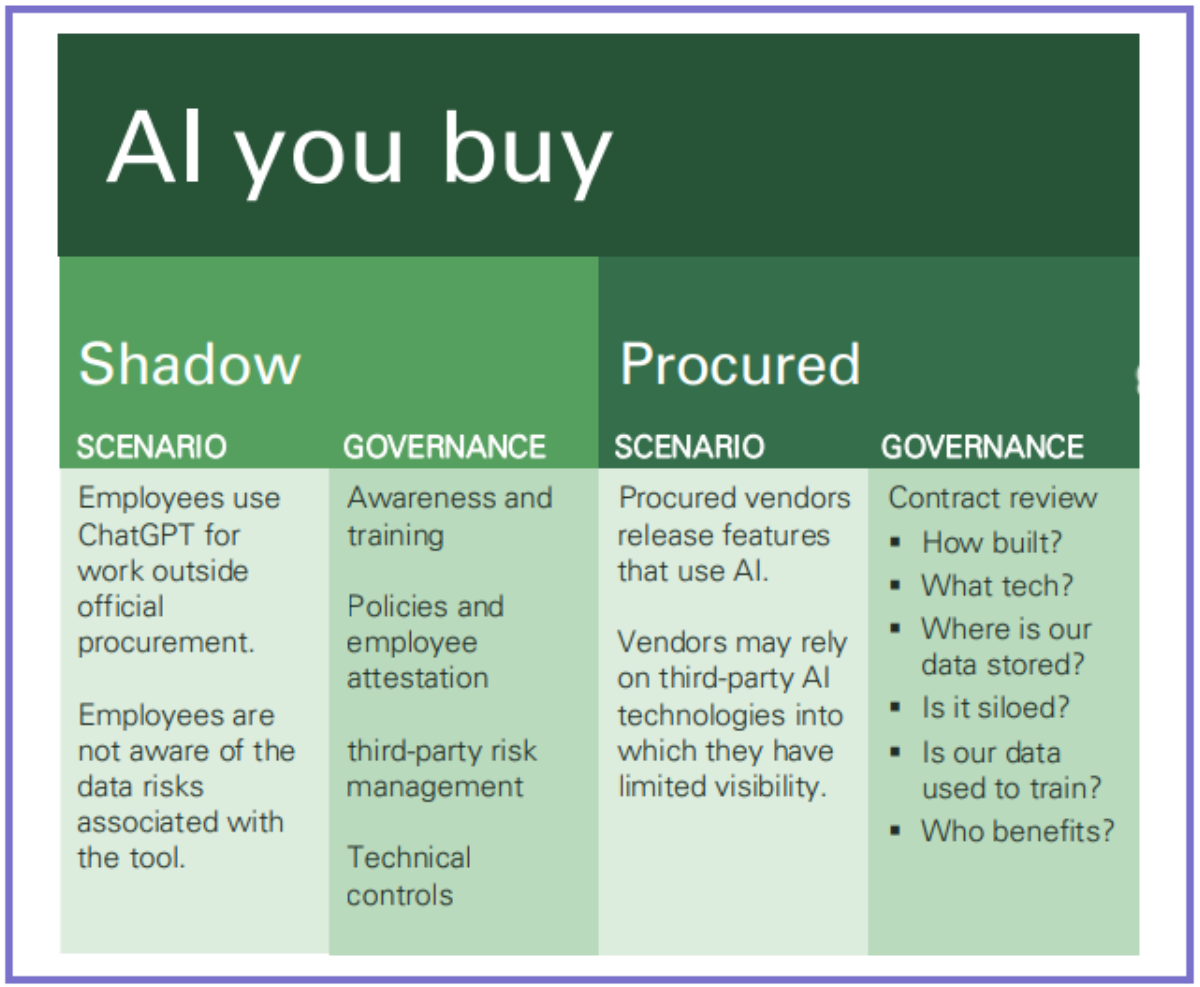
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Let's Discuss Third-Party AI Risk!

Identify	Identify Risks Associated with Third-Party AI Tools
Balance	Balance Innovation with Risk Management Strategies
Explore	Explore Governance and Controls for Third-Party AI Tools
Anticipate	Anticipate and Adapt to Evolving AI Regulations
Plan	Plan for Organizational Changes for Successful AI Adoption

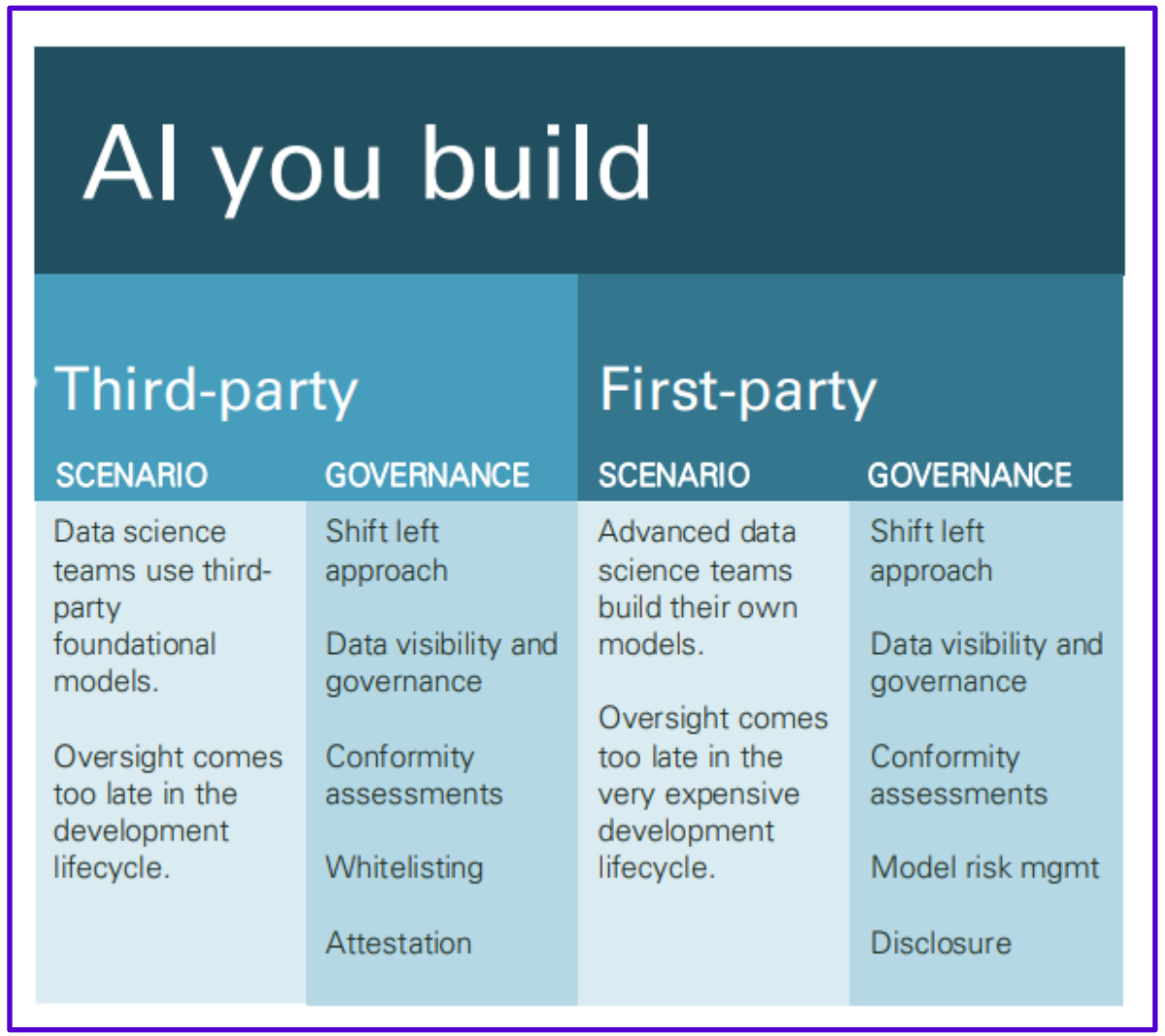
RSAC 2025 Conference

What is Third Party AI Risk?



Third Party AI Risk is..

The potential threats and challenges that arise when an organization uses AI tools, models, or services developed and operated by external vendors rather than building them in-house.



AI you build

Third-party		First-party	
SCENARIO	GOVERNANCE	SCENARIO	GOVERNANCE
Data science teams use third-party foundational models. Oversight comes too late in the development lifecycle.	Shift left approach Data visibility and governance Conformity assessments Whitelisting Attestation	Advanced data science teams build their own models. Oversight comes too late in the very expensive development lifecycle.	Shift left approach Data visibility and governance Conformity assessments Model risk mgmt Disclosure

Third Party AI Risk is..

The potential threats and challenges that arise when an organization uses AI tools, models, or services developed and operated by external vendors rather than building them in-house.

IDEAS MADE TO MATTER | ARTIFICIAL INTELLIGENCE

Third-party AI tools pose increasing risks for organizations

by Sara Brown | Sep 21, 2023

78% of organizations use third-party AI tools, with over half relying on them exclusively. However, 55% of AI failures stem from these tools. Many leaders may be unaware of all the AI tools in use—a growing issue known as "shadow AI."

FORBES > BUSINESS

BREAKING

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

Air Canada found liable for chatbot's bad advice on plane tickets

Airline's claim that online helper was responsible for its own actions was 'remarkable': small claims court

Jason Proctor · CBC News · Posted: Feb 15, 2024 12:38 PM PST | Last Updated: February 16, 2024

Workday must face novel bias lawsuit over AI screening software

By Daniel Wiessner

July 16, 2024 4:29 AM PDT · Updated 9 months ago

Tracking and classifying incidents of harm from AI

The AI Incident Tracker project classifies real-world, reported incidents by AI Risk Repository risk domain, causal factors, and harm caused.

Explore incidents | Give feedback

- Data privacy, retention, and deletion?
- Model training, validation, and maintenance?
- Information security and Privacy?
- Technology integration?
- Nth party risk ?
- Legal, regulatory, and compliance?

What's Your Top Third-Party AI Risk Concern?

What is the Top Third-Party AI Risk Concern?

Visit *www.slido.com* and input the code: **4925724**

RSAC 2025 Conference

Rethinking Risk Management for Third-Party AI

Why Does Traditional Risk Management Fall Short for Third-Party AI Tools?

Let’s Explore the AI Supply Chain Risk !

Background:

A hospital network has partnered with a third-party MedTech vendor to integrate an AI-driven diagnostic tool that analyzes medical imaging for faster, more accurate diagnoses. The AI tool is powered by data gathered from voice recognition technology developed by a separate AI company specializing in speech-to-text systems. This AI system is part of a larger healthcare supply chain that includes data suppliers, software developers, and hardware manufacturers.

Supply Chain Flow:

- Voice Recognition Developer: Supplies voice-to-text technology for transcribing patient speech in diagnostic procedures.
- MedTech Developer: Integrates the AI diagnostic tool, which uses data from both the voice recognition system and medical imagery.
- Hospital: Uses the AI-powered system in real-world medical settings to assist doctors with diagnoses.
- Patient: Receives diagnoses based on the AI’s analysis.

The AI Supply Chain Risk leads to several questions!

- Where do you sit within the supply chain?
- What are the potential risks for your organization and others?
- What level of control and assurances do you have?
- Who contributes to AI risk management in your organization?
- What processes will help you identify, mitigate, and manage risks?

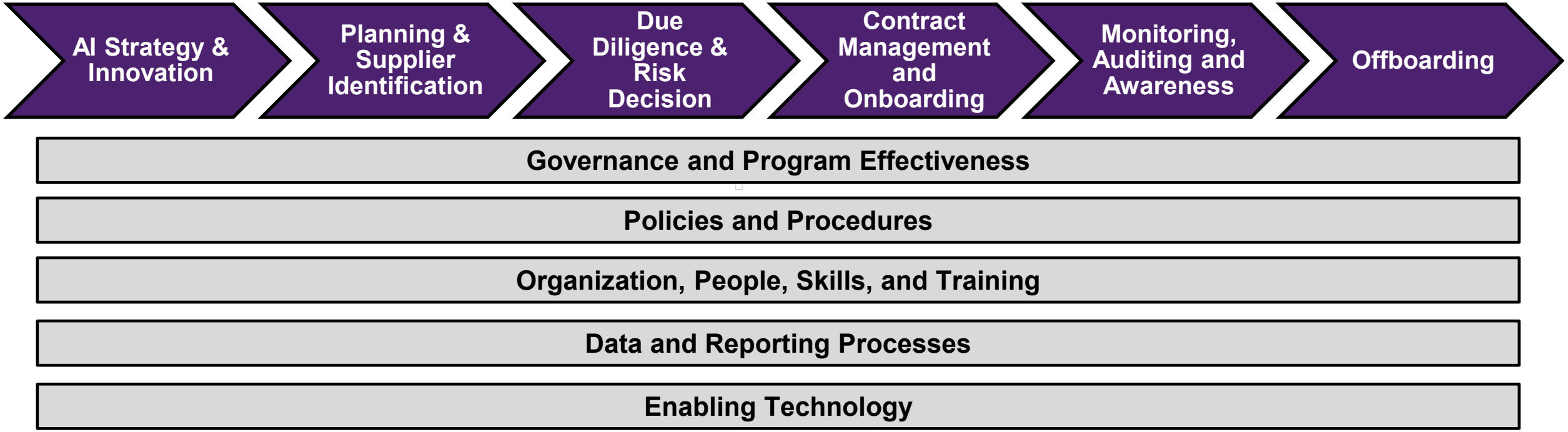
What is Different with Third Party AI Risk Management?

Aspect	Traditional TPRM	AI TPRM
Risk Focus	Financial, operational, regulatory, cyber	Adds bias, model drift, explainability, data ethics
Vendor Checks	Standard compliance (e.g., ISO, SOC 2)	AI-specific due diligence (bias testing, model metrics)
Monitoring	Periodic reviews (quarterly/annual SLAs)	Ongoing model monitoring for drift and performance anomalies
Data Handling	Data protection & encryption requirements	Deeper review of data used for AI training & outputs; Compliance requirements.
Reputational	Vendor failure can harm brand	Biased or harmful AI decisions can cause trust issues
Other	Focus on operational reliability & financial stability	Need to ensure Responsible AI, fairness, & transparency

RSAC 2025 Conference

Overview of Third-Party AI Risk Management

Third Party AI Risk Management Foundational Components



Phase 1: AI Strategy & Innovation

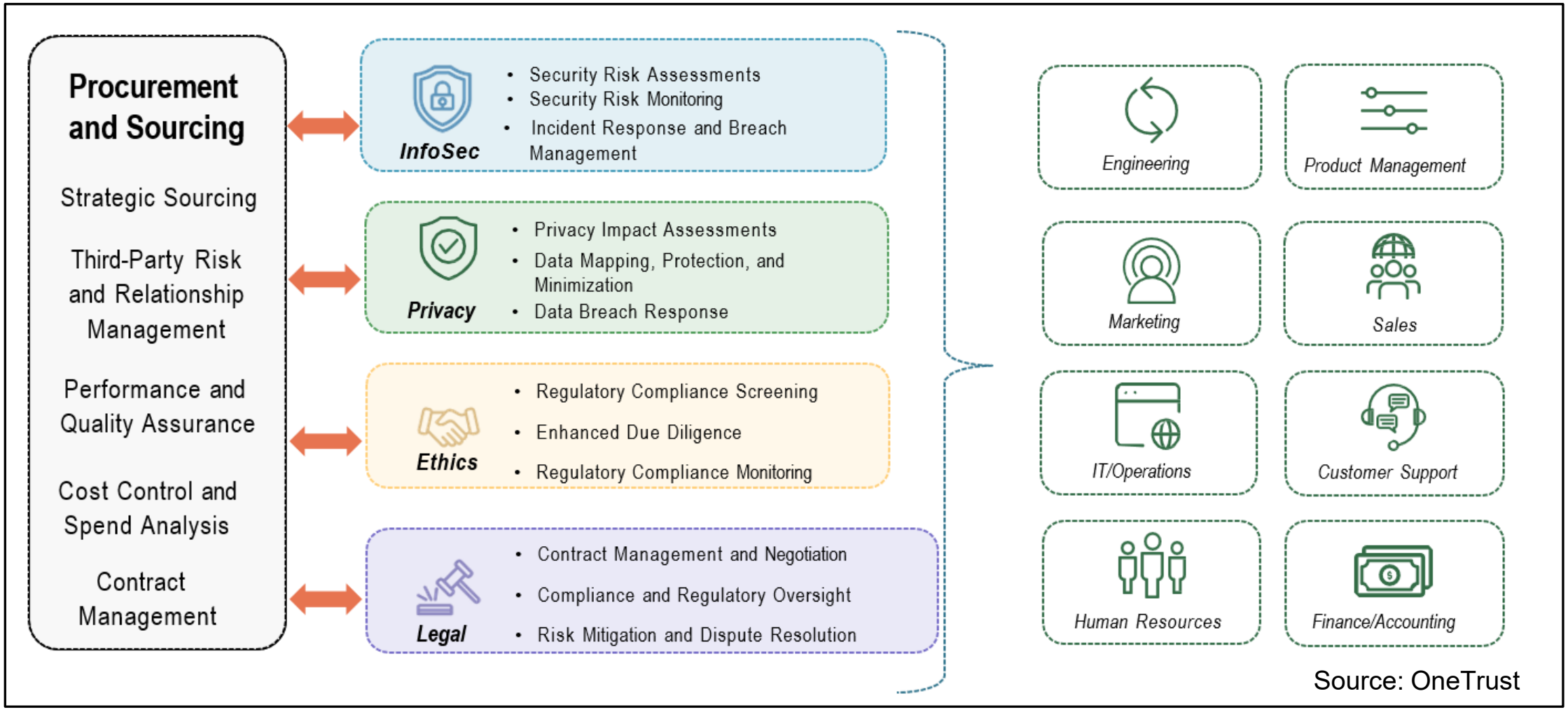
Scenario: Purchasing an AI-Driven Risk Management SaaS

You're evaluating a vendor that offers a SaaS platform for risk management. This tool uses AI/ML algorithms to prioritize risks, detect anomalies, and predict emerging threats.

How would you apply this framework to assess and manage the AI-related risks of this tool?

- **Needs Identification:** Identifies a pain point e,g, limited visibility into emerging risks
- **Define Business Case**: Why is AI-driven risk management tool is needed?
- **Establish Ownership:** Assign an AI risk owner for this initiative.
- **Align with Policies & Ethics**: Ensure the use of AI aligns with internal policies (Responsible AI guidelines) and any mandated regulations (GDPR, industry standards).
- **Innovation Committee Input**: A cross-functional team (risk, IT, compliance, business) reviews early results to decide whether to move forward.

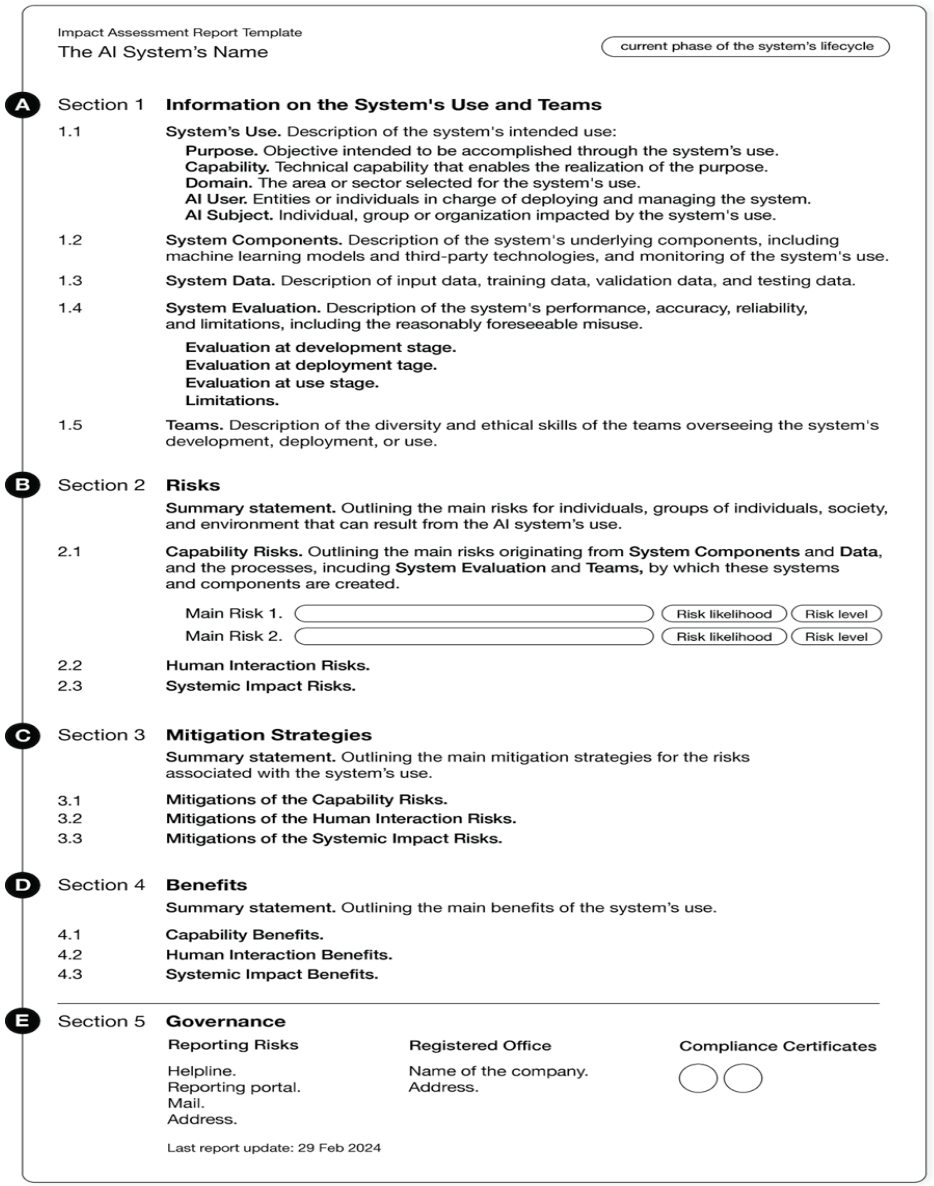
Phase 2:Planning and Supplier Identification



Source: OneTrust

Phase 3: Due Diligence Parameters

- Capabilities & Limitations
- Training, Validation, & Testing Datasets
- Testing & Quality Assurance
- Supply Chain Dependencies
- Compliance with Standards
- Privacy & Security
- Guidelines for Use



Impact Assessment Report Template
The AI System's Name
current phase of the system's lifecycle

A Section 1 **Information on the System's Use and Teams**

1.1 **System's Use.** Description of the system's intended use:
Purpose. Objective intended to be accomplished through the system's use.
Capability. Technical capability that enables the realization of the purpose.
Domain. The area or sector selected for the system's use.
AI User. Entities or individuals in charge of deploying and managing the system.
AI Subject. Individual, group or organization impacted by the system's use.

1.2 **System Components.** Description of the system's underlying components, including machine learning models and third-party technologies, and monitoring of the system's use.

1.3 **System Data.** Description of input data, training data, validation data, and testing data.

1.4 **System Evaluation.** Description of the system's performance, accuracy, reliability, and limitations, including the reasonably foreseeable misuse.
Evaluation at development stage.
Evaluation at deployment tage.
Evaluation at use stage.
Limitations.

1.5 **Teams.** Description of the diversity and ethical skills of the teams overseeing the system's development, deployment, or use.

B Section 2 **Risks**

Summary statement. Outlining the main risks for individuals, groups of individuals, society, and environment that can result from the AI system's use.

2.1 **Capability Risks.** Outlining the main risks originating from **System Components** and **Data**, and the processes, incuding **System Evaluation** and **Teams,** by which these systems and components are created.

Main Risk 1. Risk likelihood Risk level
Main Risk 2. Risk likelihood Risk level

2.2 **Human Interaction Risks.**
2.3 **Systemic Impact Risks.**

C Section 3 **Mitigation Strategies**

Summary statement. Outlining the main mitigation strategies for the risks associated with the system's use.

3.1 **Mitigations of the Capability Risks.**
3.2 **Mitigations of the Human Interaction Risks.**
3.3 **Mitigations of the Systemic Impact Risks.**

D Section 4 **Benefits**

Summary statement. Outlining the main benefits of the system's use.

4.1 **Capability Benefits.**
4.2 **Human Interaction Benefits.**
4.3 **Systemic Impact Benefits.**

E Section 5 **Governance**

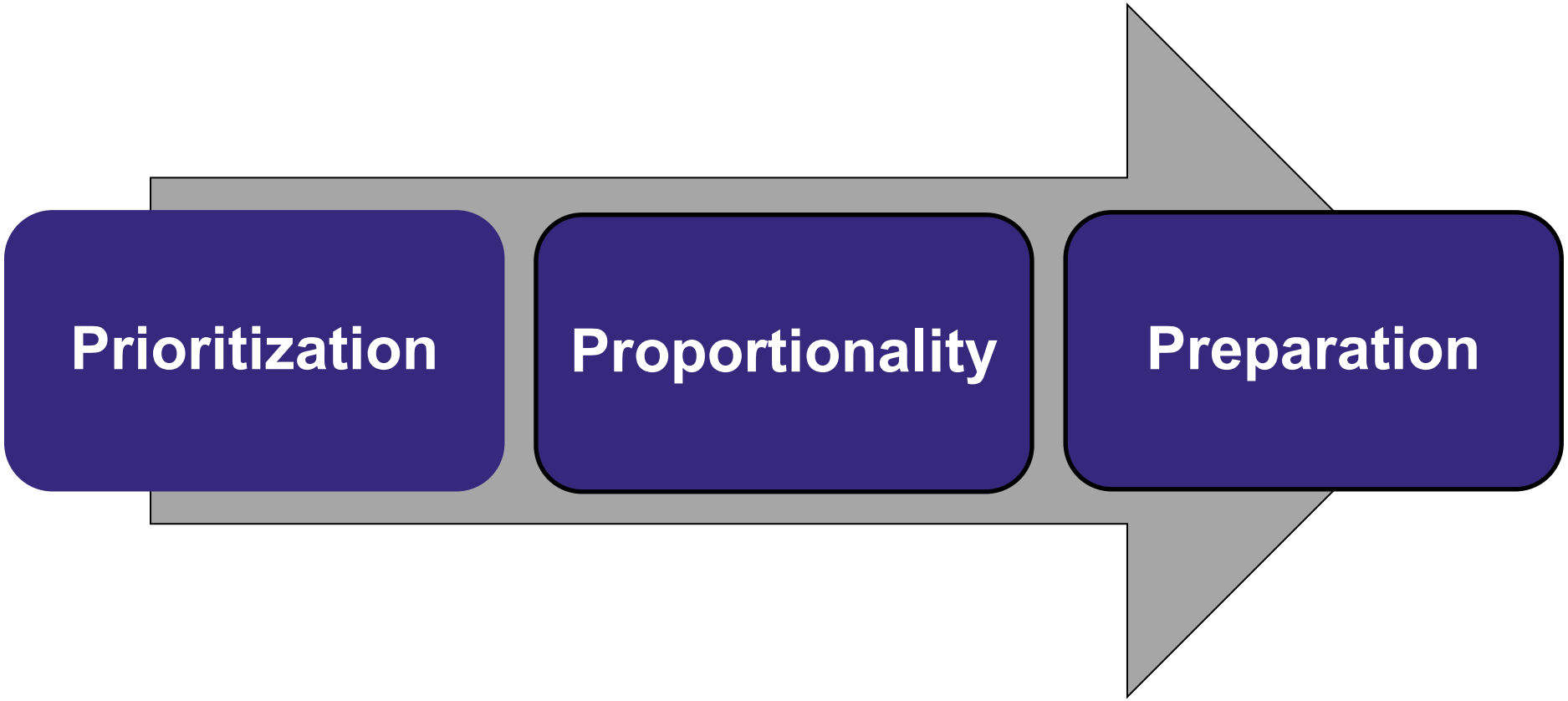
Reporting Risks	Registered Office	Compliance Certificates
Helpline. Reporting portal. Mail. Address.	Name of the company. Address.	

Last report update: 29 Feb 2024

Phase 3: AI Impact Assessment

- Capture an AI system's risk
- Cover full development life-cycle requirements
- Assess impact & increase accountability through a multi-stakeholder analysis
- Facilitate go/no-go decisions
- Record & track risks

Phase 3: Due Diligence and Risk Decision



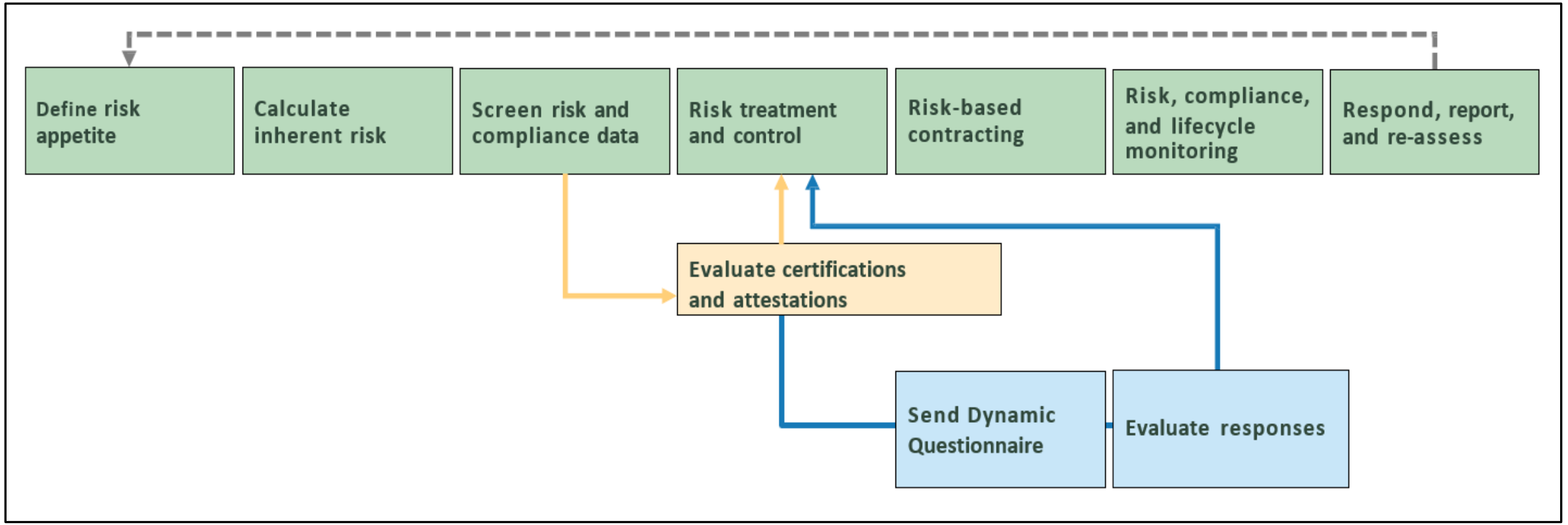
The higher the risks, the greater the due diligence…

Phase 4: Contract Management and Onboarding

Risk-based contracting allows businesses to structure agreements based on the allocation of risk and rewards between parties.

- Performance standards or service level agreements (SLAs)
- Security & confidentiality provisions
- Due diligence language
- Standard Contractual Clauses (SCCs)
- Term & pricing methods
- Exit strategy

Phase 4: Contract Management and Onboarding



Phase 5: Monitoring, Auditing and Awareness

Continuously Monitor Vendor Performance and Risk Profile Changes

Business context:

Lifecycle stage & processes

Contract renewal:

Expiration dates & SLAs

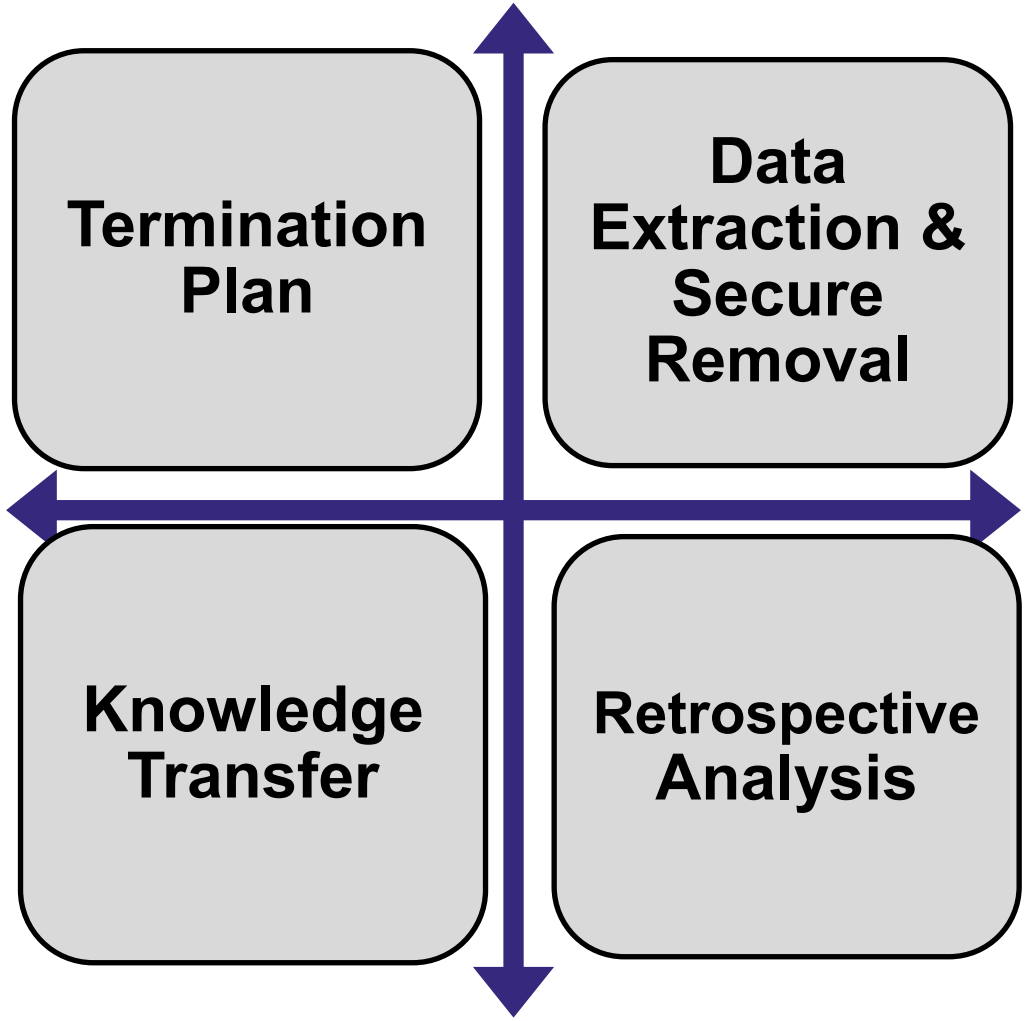
Changes in scope:

Vendor service enhancements

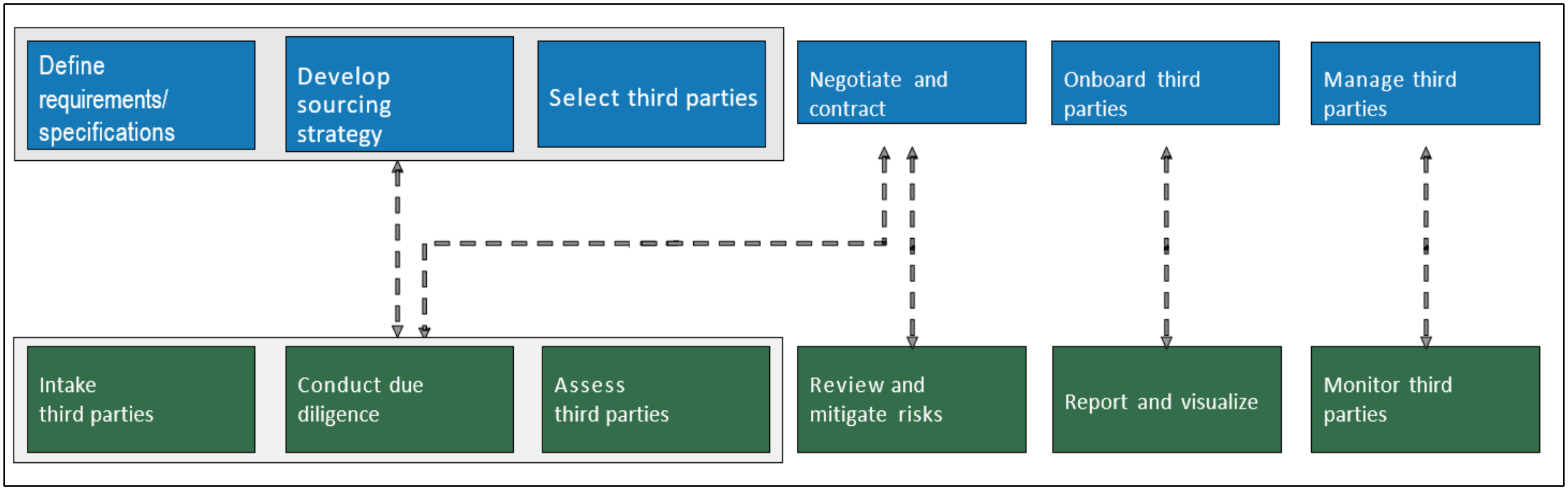
Third-Party Risk Ratings:

Risk ratings & monitoring lists

Phase 6: Offboarding



Key Takeaway:
Alignment is Required Across Multiple Functions!



Key Takeaway:
Future-Proof Your Relationships

Key Master Services Agreement Clauses:

- Terms & Duration: Defines the agreement's start/end dates, renewal terms, and early termination procedures.
- Dispute Resolution: Outlines methods (negotiation, mediation, arbitration, or litigation) to resolve conflicts.
- Amendment & Modification: Establishes how the MSA can be updated, including the need for mutual consent.
- Severability: Ensures remaining clauses stand if one part is deemed invalid or unenforceable.
- Force Majeure: Clarifies how unexpected events beyond either party's control are addressed.

RSAC 2025 Conference

Anticipate and Adapt to Evolving AI Regulations

AI Regulations Globally

AI Governance:
Frameworks and guardrails that are necessary to ensure that AI is developed and used in a responsible manner

Responsible AI:
Ethical considerations that are integrated into the development and deployment of AI systems

Your Compliance Obligations Depends On…

AI you acquire

SHADOW

SCENARIO	GOVERNANCE
Employees use ChatGPT for work outside official procurement. Employees are not aware of the data risks associated with the tool.	Awareness and training Policies and employee attestation Third party risk management Technical controls

PROCURED

SCENARIO	GOVERNANCE
Procured vendors release features that use AI. Vendors may rely on third-party AI technologies into which they have limited visibility.	Contract review • How built? • What tech? • Where is our data stored? • Is it siloed? • Is our data used to train? • Who benefits?

AI you build

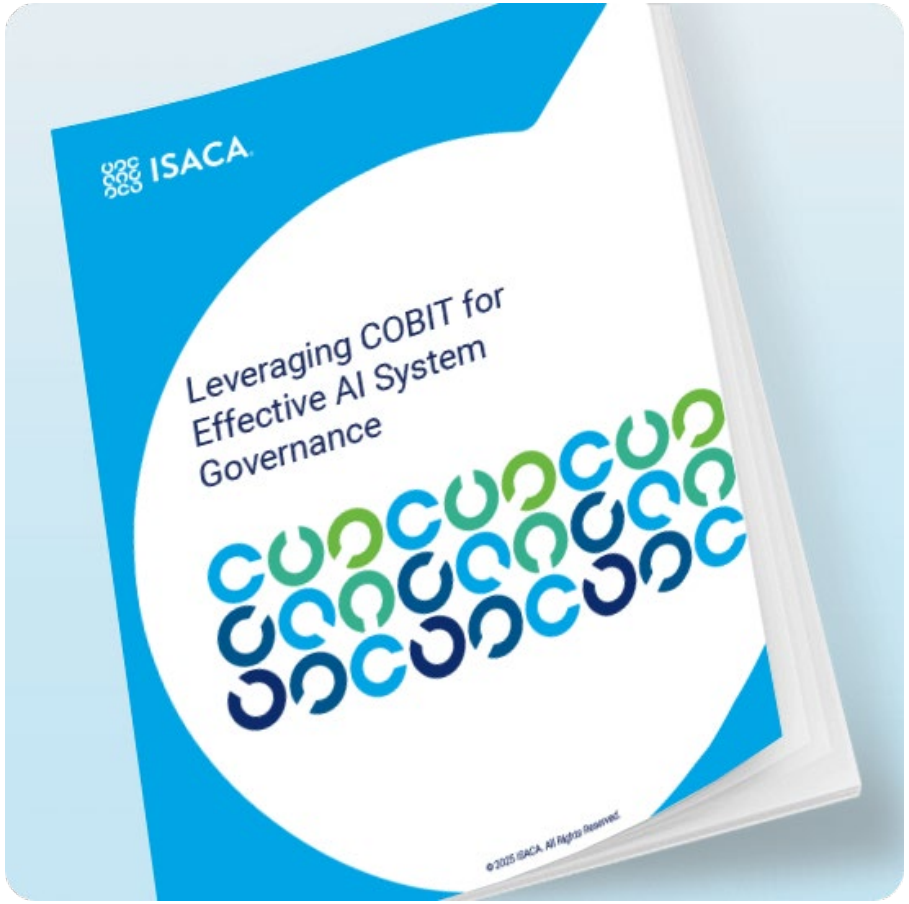
THIRD-PARTY

SCENARIO	GOVERNANCE
Data science teams use third-party foundational models. Oversight comes too late in the development lifecycle.	Shift left approach Data visibility and governance Conformity assessments Whitelisting Attestation

FIRST-PARTY

SCENARIO	GOVERNANCE
Advanced data science teams build their own models. Oversight comes too late in the very expensive development lifecycle.	Shift left approach Data visibility and governance Conformity assessments Model risk mgmt Disclosure

COBIT for AI Governance



As AI technology continues to evolve, so will the need for adaptive governance frameworks.

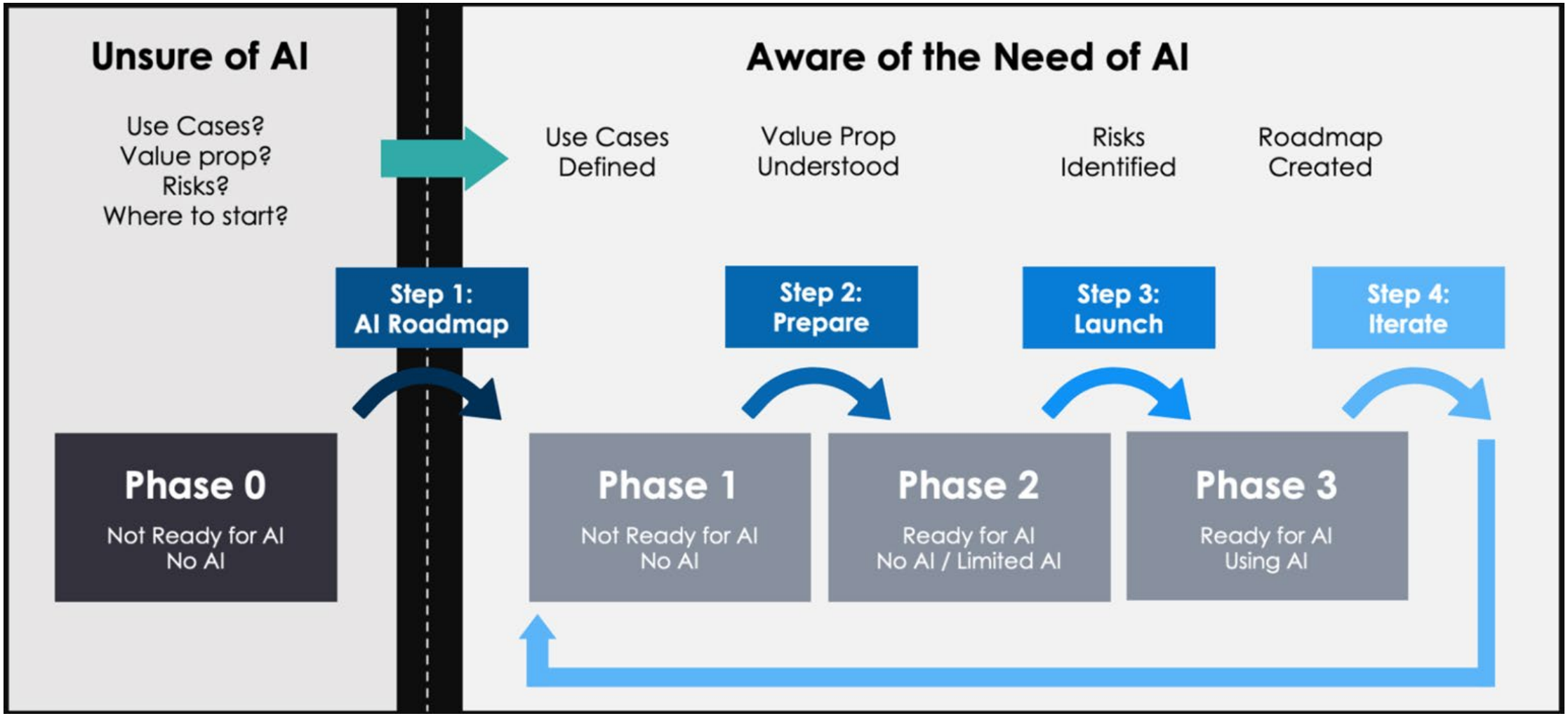
The COBIT framework can address the gaps by offering a holistic approach to AI governance.

Its primary goal is to help organizations align IT with business objectives, manage risk, and ensure the optimal use of resources

RSAC 2025 Conference

Organizational and Cultural Changes for Successful AI Adoption

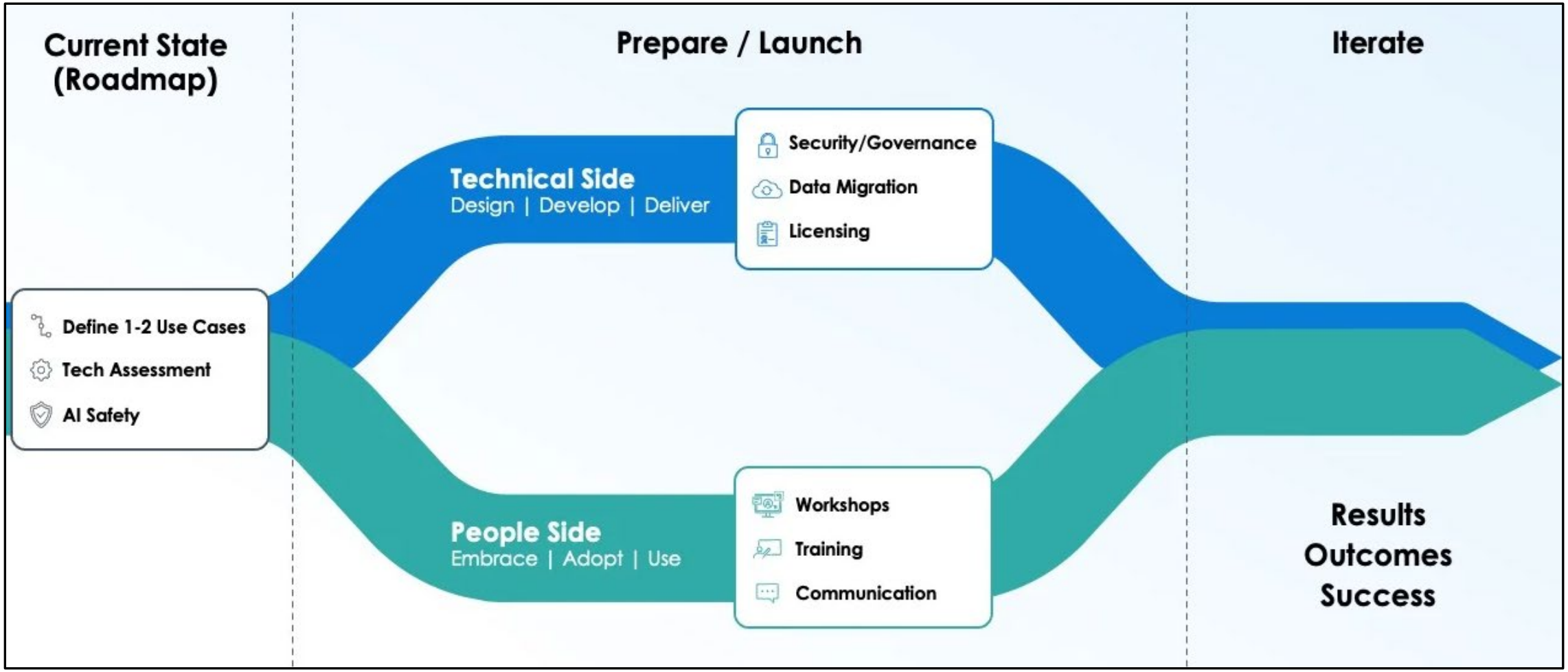
What is Your AI Readiness?



Organizational and Cultural Changes for Successful AI Adoption

Visit www.slido.com and input the code:
4925724

Managing Organizational Change



RSAC 2025 Conference

Key Takeaways

Key Takeaways

Address	Unique AI Risks: Address bias, model drift, and data issues.
Involve	Cross-Functional Collaboration: Involve legal, IT, compliance, and business teams.
Assess	Continuous Monitoring: Regularly assess AI performance and compliance.
Set	Clear Contracts: Set expectations for AI performance and breach management.
Align	Ethical & Regulatory Compliance: Align with evolving standards and laws.
Identify and manage	Proactive Risk Mitigation: Identify and manage risks early in the process.

RSAC | 2025 Conference

Many Voices.
One Community.

Mary Carmichael CPA CMA, CISM, CISA, CRISC, PRSOCI

https://www.linkedin.com/in/carmichaelmary/

Dooshima Dabo'Adzuana CRISC, COBIT, Cert CII UK, ISO/IEC 42001 PI

https://www.linkedin.com/in/dooshima-dabo-adzuana/